

# ARITHMETIC OF DIVISION FIELDS

ARMAND BRUMER AND KENNETH KRAMER

**ABSTRACT.** We study the arithmetic of division fields of semistable abelian varieties  $A/\mathbb{Q}$ . The Galois group of  $\mathbb{Q}(A[2])/\mathbb{Q}$  is analyzed when the conductor is odd and squarefree. The irreducible semistable mod 2 representations of small conductor are determined under GRH. These results are used in *Paramodular abelian varieties of odd conductor*, arXiv:1004.4699.

## 1. INTRODUCTION

This note contains results needed in [BK2] and of independent interest. We write  $S$  for a set of primes,  $N_S$  for their product and  $\ell$  for a prime not in  $S$ . If  $F/\mathbb{Q}$  is Galois,  $\mathcal{I}_v(F/\mathbb{Q})$  denotes the inertia group at a place  $v$  of  $F$ .

**Definition 1.1** ([BK1]). The Galois extension  $F/\mathbb{Q}$  is  $(\ell, N_S)$ -controlled if

- i)  $F/\mathbb{Q}$  is unramified outside  $S \cup \{\ell, \infty\}$ ;
- ii)  $\mathcal{I}_v(F/\mathbb{Q}) = \langle \sigma_v \rangle$  is cyclic of order  $\ell$  for all ramified  $v$  not over  $\ell$ ;
- iii)  $\mathcal{I}_\lambda(F/\mathbb{Q})^u = 1$  for all  $u > 1/(\ell - 1)$  and  $\lambda$  over  $\ell$ , using the upper numbering of Serre as in §5.

We denote by  $V$  a finite dimensional vector space over the finite field  $\mathbb{F}$  of characteristic  $\ell$  with  $q = |\mathbb{F}|$ . Additional structure on  $V$ , such as a symplectic pairing or Galois action, is often imposed.

**Definition 1.2.** Let  $V$  be an  $\mathbb{F}[G_{\mathbb{Q}}]$ -module and  $F = \mathbb{Q}(V)$ . The set  $S$  of rational primes  $p \neq \ell$  ramified in  $F/\mathbb{Q}$  comprises the *bad primes* of  $V$ . Declare  $V$  *semistable* if  $F$  is  $(\ell, N_S)$ -controlled and  $(\sigma_v - 1)^2(V) = 0$  for all  $v$  lying over the primes of  $S$ .

Throughout,  $A/\mathbb{Q}$  is a semistable abelian variety with good reduction at  $\ell$  and  $\text{End}_{\mathbb{Q}} A = \mathfrak{o}$  is the ring of integers in a totally real number field. If  $\mathfrak{l}$  is a prime over  $\ell$  in  $\mathfrak{o}$  and  $\mathfrak{o}/\mathfrak{l} = \mathbb{F}$ , then  $V = A[\mathfrak{l}]$  is semistable [Gro, Fo]. The conductor of  $A$  has the form  $N_A = N^d$  with  $d = [\mathfrak{o} : \mathbb{Z}]$ . Since inertia over each bad prime  $p$  is tame,

$$(1.3) \quad \text{ord}_p(N) = \dim_{\mathbb{F}} V/V^{\mathcal{I}} = \dim_{\mathbb{F}} (\sigma_v - 1)V.$$

In §2, we use known results on symplectic representations generated by transvections to describe  $\text{Gal}(\mathbb{Q}(W)/\mathbb{Q})$  for constituents  $W$  of  $V$  with squarefree conductor, assuming  $\mathfrak{l}$  lies over 2.

A *stem field* for a Galois extension  $F/k$  is an intermediate field  $K$  whose Galois closure over  $k$  is  $F$ . If  $G = \text{Gal}(F/k)$  acts faithfully and transitively on a set  $X$ , the fixed field of the stabilizer  $G_x$  of any  $x$  in  $X$  is a stem field. A formula for

---

*Date:* February 21, 2011.

*2010 Mathematics Subject Classification.* Primary 11F80; Secondary 11S15, 11G10, 11Y40.

*Key words and phrases.* semistable Galois representation, transvection, stem field discriminant, bounded ramification.

Research of the second author partially supported by NSF grant DMS 0739346.

the discriminant  $d_{K/k}$  is given in §3 and applied to semistable Galois modules. By relating number-theoretic properties of  $K$  and  $F$ , certain computations become feasible, since  $K$  has smaller degree and discriminant than  $F$ .

Suppose  $E/\mathbb{Q}_\ell$  is a Galois extension of  $\ell$ -adic fields satisfying (1.1iii). In §5, we find conditions on the ray class conductor of an abelian extension  $L/E$  so that (1.1iii) also holds for the Galois closure of  $L/\mathbb{Q}_\ell$ . The maximal  $(2, N)$ -controlled extension for all odd  $N \leq 79$  and for  $N = 97$ , is determined in §6, thanks to §5 and Odlyzko's GRH bounds. We also construct a  $(2, 127)$ -controlled extension of degree 161280 with root discriminant just above the asymptotic Odlyzko bound, but finiteness of a maximal one is unknown.

A finite flat group scheme  $\mathcal{V}$  over  $\mathbb{Z}_\ell$  admits a filtration  $0 \subseteq \mathcal{V}^m \subseteq \mathcal{V}^0 \subseteq \mathcal{V}$  with connected component  $\mathcal{V}^0$ , étale quotient  $\mathcal{V}^{et} = \mathcal{V}/\mathcal{V}^0$ , multiplicative subscheme  $\mathcal{V}^m$  and biconnected subquotient  $\mathcal{V}^b = \mathcal{V}^0/\mathcal{V}^m$ . Let  $\lambda$  be a place over  $\ell$  in  $F = \mathbb{Q}(V)$  and  $\mathcal{D}_\lambda$  its decomposition group. We denote the corresponding  $\mathbb{F}[\mathcal{D}_\lambda]$ -modules of  $F_\lambda$ -valued points by  $V$ ,  $V^{et}$ ,  $V^m$  and  $V^b$ , respectively.

**Definition 1.4** ([BK2]).  $A/\mathbb{Q}$  is  $\mathfrak{o}$ -paramodular if  $\dim A = 2d$ , with  $d = [\mathfrak{o}:\mathbb{Z}]$ .

Let  $A$  be  $\mathfrak{o}$ -paramodular, with  $\mathfrak{o}/\mathfrak{l} \simeq \mathbb{F}_2$ . When  $A[\mathfrak{l}]$  is irreducible, estimates for the discriminant of a stem field of  $\mathbb{Q}(A[\mathfrak{l}])$  are obtained in §4. The reducible case leads to ray class fields whose conductors are controlled by the results of §5. This information depends on the structure of  $A[\mathfrak{l}]$  as a group scheme and is used in [BK2].

Concluding questions and comments appear in §7.

## 2. MOD 2 REPRESENTATIONS GENERATED BY TRANSVECTIONS

A *transvection* on  $V$  is an automorphism of the form  $\tau(x) = x + \psi(x)z$ , with  $\psi : V \rightarrow \mathbb{F}$  a nonzero linear form and  $z \neq 0$  in  $\ker \psi$ . Assume  $V$  admits a non-degenerate alternating pairing  $[\cdot, \cdot] : V \times V \rightarrow \mathbb{F}$  preserved by  $\tau$  and let  $\dim V = 2n$ . Then  $\tau(x) = x + a[z, x]z$  for some  $z \in V$  and  $a \in \mathbb{F}^\times$ . When  $a$  is a square in  $\mathbb{F}$ , we may take  $a = 1$ . For  $x$  and  $z$  in  $V$ , define  $\tau_{[z]}$  by

$$(2.1) \quad \tau_{[z]}(x) = x + [z, x]z.$$

Assume that  $\ell = 2$  for the rest of this section, unless otherwise noted.

A quadratic form  $\theta$  on the symplectic space  $V$  is called a *theta characteristic* if  $\theta(x+y) = \theta(x) + \theta(y) + [x, y]$  for all  $x, y$  in  $V$ . Theta characteristics form a principal homogeneous space over  $V$ , with  $(\theta + a)(x) = \theta(x) + [a, x]^2$  for  $a$  in  $V$ . We identify  $a$  with  $[a, -]$  under the Galois isomorphism  $V \simeq \text{Hom}_{\mathbb{F}}(V, \mathbb{F})$ . Elements  $\sigma$  in  $\text{Sp}(V)$  act by  $\sigma(\theta)(x) = \theta(\sigma(x))$ . Then  $\sigma(\theta + a) = \sigma(\theta) + \sigma(a)$  and

$$(2.2) \quad \tau_{[z]}(\theta) = \theta + \sqrt{1 + \theta(z)}z.$$

Fix a symplectic basis  $\{e_1, \dots, e_{2n}\}$  for  $V$  with  $[e_i, e_j] = 1$  if  $|i - j| = n$  and 0 otherwise. Let  $\wp(x) = x^2 - x$  be the Artin-Schreier function. Depending on whether or not the Arf invariant  $\text{Arf}(\theta) = \sum_i \theta(e_i)\theta(e_{i+n})$  vanishes in  $\mathbb{F}/\wp(\mathbb{F})$ , we say  $\theta$  is even or odd and write  $O_{2n}^\pm$  for the corresponding orthogonal group. Further,  $\text{Sp}(V)$  acts transitively on the sets  $\Theta_{2n}^\pm$  of even and odd characteristics and

$$(2.3) \quad |\Theta_{2n}^\pm| = \frac{1}{2}q^n(q^n \pm 1).$$

Denote the symmetric, alternating, dihedral and cyclic groups by  $\mathcal{S}_n$ ,  $\mathcal{A}_n$ ,  $D_n$ ,  $C_n$  respectively.

**Proposition 2.4** ([McL]). *If  $\mathbb{F} = \mathbb{F}_2$  and  $G \subsetneq \mathrm{SL}(V)$  is an irreducible subgroup generated by transvections, then  $\dim V = 2n$  with  $n \geq 2$  and  $G$  is  $O_{2n}^\pm(\mathbb{F}_2)$ ,  $\mathrm{Sp}_{2n}(\mathbb{F}_2)$  or  $\mathcal{S}_m$  with  $2n+1 \leq m \leq 2n+2$ . Also,  $G$  has trivial center and is self-normalizing in  $\mathrm{SL}(V)$ .*

**Proposition 2.5.** *Let  $V$  be a symplectic space of dimension  $2n$ . An irreducible subgroup  $G$  of  $\mathrm{Sp}(V)$  generated by transvections is one of the following, with  $\mathbb{F}' \subseteq \mathbb{F}$ :*

- i) *dihedral,  $D_m$  with  $m$  dividing one of  $|\mathbb{F}| \pm 1$  and  $n = 1$ ;*
- ii) *orthogonal,  $O_{2n}^\pm(\mathbb{F}')$  for  $n \geq 2$ ;*
- iii) *symplectic,  $\mathrm{Sp}_{2n}(\mathbb{F}')$ ;*
- iv) *symmetric,  $\mathcal{S}_m$  for  $n \geq 2$  and  $2n+1 \leq m \leq 2n+2$ .*

*Moreover,  $G$  has trivial center and is self-normalizing in  $\mathrm{Sp}(V)$ .*

*Proof.* If  $V$  is imprimitive, then  $V$  is monomial [Zal], say  $V = \mathrm{Ind}_{H_1}^G(V_1)$ , with  $V_1 = \mathbb{F}e_1$  and  $[G : H_1] = \dim V = 2n$ . Arrange that  $G = \cup g_i H_1$ , with  $g_1 = 1$  and  $V_i = g_i(V_1) = \mathbb{F}e_i$ , and let  $\pi : G \rightarrow \mathcal{S}_{2n}$  by  $gV_i = V_{\pi(g)i}$ . Since  $\pi(G)$  is transitive and generated by transpositions, namely the images of the transvections,  $\pi(G) = \mathcal{S}_{2n}$ . For  $h$  in  $H = \ker \pi$ , we have  $he_i = \chi_i(h)e_i$  and so the pairing on  $V$  satisfies  $[e_i, e_j] = [he_i, he_j] = \chi_i(h)\chi_j(h)[e_i, e_j]$ . Hence  $[e_i, e_j] = 0$  or  $\chi_i(h)\chi_j(h) = 1$ . Because the pairing is perfect and  $\pi(G)$  is doubly transitive, we must have  $[e_i, e_j] \neq 0$  and  $\chi_i(h)\chi_j(h) = 1$  for all  $i \neq j$ . If  $n \geq 2$ , then  $\chi_i(H) = 1$  for all  $i$ ,  $H = 1$  and  $\pi$  is an isomorphism. The stabilizer  $H_1$  of  $V_1$  is isomorphic to  $\mathcal{S}_{2n-1}$  and so the character  $\chi_1 : H_1 \rightarrow \mathbb{F}^\times$  is trivial. Since  $\sum g_i(e_1)$  is a non-trivial fixed point,  $V$  is reducible. Now combine [HBI, Ch. II, §8.27] and [Kan, KM] to get our list.

If  $g$  in  $\mathrm{Sp}_{2n}(\mathbb{F})$  normalizes  $G$  and  $\sigma$  is in  $\mathrm{Gal}(\mathbb{F}/\mathbb{F}')$ , then  $g^\sigma g^{-1}$  centralizes  $G$ . Our representations are absolutely irreducible and the center of  $\mathrm{Sp}_{2n}(\mathbb{F})$  is trivial, so  $g$  is in  $\mathrm{Sp}_{2n}(\mathbb{F}')$ . To verify that the center is trivial and  $G = \mathcal{S}_m$  is self-normalizing in  $\mathrm{Sp}_{2n}(\mathbb{F}_2)$  when  $m \neq 6$ , use the fact that all automorphisms are inner and absolute irreducibility. Note that  $\mathcal{S}_6 \simeq \mathrm{Sp}_4(\mathbb{F}_2)$ . The dihedral case is easily checked. See [Dye] for the other cases.  $\square$

**Remark 2.6.** As to (iv) above, note that  $\mathcal{S}_m$  acts by permutation on

$$Y = \{(a_1, \dots, a_m) \in \mathbb{F}_2^m \mid a_1 + \dots + a_m = 0\}$$

with pairing  $[(a_i), (b_i)] = \sum a_i b_i$ . Let  $V = Y/\langle(1, \dots, 1)\rangle$  or  $V = Y$  according as  $m$  is even or odd. Then  $V$  is irreducible and transpositions in  $\mathcal{S}_m$  correspond to transvections on  $V$ . This action of  $\mathcal{S}_m$  and that of Galois on  $J[2]$  for a hyperelliptic Jacobian are compatible.

**Lemma 2.7.** *Let  $V$  be an irreducible  $\mathbb{F}[G]$ -module and let  $P$  be the subgroup of  $G$  generated by transvections. If  $P$  is not trivial, then  $V|_P$  is the direct sum of  $r$  irreducible  $\mathbb{F}[P]$ -modules  $W_i$  and  $P = Q_1 \cdots Q_r$  is a direct product, with  $Q_i = \langle \sigma \in P \mid \sigma|_{W_i} \text{ is a transvection and } \sigma|_{W_j} = 1 \text{ for all } j \neq i \rangle$ . If  $V$  is symplectic, then the  $W_i$  are symplectic and the sum is orthogonal.*

*Proof.* Since  $P$  is normal, Clifford's theorem applies. Let  $W_1$  be an irreducible submodule of  $V|_P$ ,  $H = \{h \in G \mid h(W_1) \simeq W_1 \text{ as } P\text{-module}\}$  and  $X = \sum_{h \in H} h(W_1)$ . Then  $V = \mathrm{ind}_H^G(X)$  and  $X|_P \simeq eW_1$  is isotypic. If  $G = \cup_1^r g_i H$  is a coset decomposition with  $g_1 = 1$ , then  $V|_P \simeq \oplus_1^r eW_i$  with  $W_i = g_i(W_1)$ . For any transvection  $\tau$ , we have  $1 = \dim(\tau - 1)(V) = e \sum_1^r \dim(\tau - 1)(W_i)$ . Thus  $e = 1$  and  $\tau$  is in  $Q_i$  for

a unique index  $i$ . Moreover  $Q_i = g_i Q_1 g_i^{-1}$  is normal in  $P$  and  $P = Q_1 \cdots Q_r$  is a direct product.

Now suppose  $V$  symplectic and  $\tau$  a transvection in  $Q_i$ . Then  $(\tau - 1)W_i = \langle z \rangle$  with  $z$  in  $W_i \cap W_j^\perp$  for all  $j \neq i$ , but not in  $W_i^\perp$ . Irreducibility of  $W_i$  implies that  $W_i \subseteq W_j^\perp$  and  $W_i \cap W_i^\perp = 0$ . Hence  $W_i$  is symplectic.  $\square$

**Proposition 2.8.** *Let  $V$  be an irreducible symplectic  $\mathbb{F}[G_{\mathbb{Q}}]$ -module with squarefree conductor  $N$  and let  $F = \mathbb{Q}(V)$ . Let  $P$  be the subgroup of  $G = \text{Gal}(F/\mathbb{Q})$  generated by transvections. If  $P = G$ , then  $G$  is as in Prop. 2.5.*

*Otherwise,  $V = \text{ind}_P^G W$  and  $G \simeq Q \wr C_2$ , where  $Q$  is in the list in Prop. 2.5. Moreover  $F^P = \mathbb{Q}(i)$  and  $N = \mathfrak{n}\bar{\mathfrak{n}}$  in  $\mathbb{Z}[i]$ , where  $\mathfrak{n}$  generates the conductor ideal of  $W$  as  $\mathbb{F}[G_{\mathbb{Q}(i)}]$ -module.*

*Proof.* Since  $\text{ord}_{p_v}(N) = 1$ , any generator  $\sigma_v$  of  $\mathcal{I}_v(F/\mathbb{Q})$  is a transvection. Prop. 6.2 shows that the fixed field  $F^P = \mathbb{Q}(i)$ . The restriction  $V|_P$  is reducible by Lemma 2.5 and so  $V$  is induced. Hence  $H = P \simeq Q_1 \times Q_2$  and  $G \simeq Q_1 \wr C_2$  is a wreath product, thanks to Lemma 2.7. The conductor formula for an induced module gives  $N = \mathfrak{n}\bar{\mathfrak{n}}$ , where  $\mathfrak{n} \in \mathbb{Z}[i]$  is the odd part of the Artin conductor of  $W$ , since  $\mathbb{Q}(i)$  is unramified at odd places.  $\square$

**Remark 2.9.** In Prop. 2.8, if we take  $\mathbb{F} = \mathbb{F}_2$  but do not assume  $V$  symplectic, the conclusions obtain, with “Prop. 2.5” replaced by “Prop. 2.4.”

**Remark 2.10.** The conjugacy class of any involution  $\sigma$  in  $\text{Sp}(V)$  has invariants  $t = \text{rank}(\sigma - 1)$  and  $\delta$ , with  $\delta = 0$  if  $[v, (\sigma - 1)v] = 0$  for all  $v$  in  $V$ , and  $\delta = 1$  otherwise. If  $t = n$  and  $\sigma$  is in  $O_{2n}^-(\mathbb{F})$ , then  $\delta = 1$ . If  $t$  is odd, then  $\delta = 1$ .

For the last result in this section,  $\ell = 3$ .

**Proposition 2.11.** *Let  $V$  be an irreducible symplectic  $\mathbb{F}_3[G_{\mathbb{Q}}]$ -module with square-free conductor  $N$ . Set  $2n = \dim_{\mathbb{F}} V$ ,  $F = \mathbb{Q}(V)$  and  $G = \text{Gal}(F/\mathbb{Q})$ . Then*

- i)  $G \simeq \text{GSp}_{2n}(\mathbb{F}_3)$  or
- ii)  $n$  is even,  $G \simeq \text{Sp}_n(\mathbb{F}_3) \wr C_2$  and  $N = \mathfrak{n}\bar{\mathfrak{n}}$  in  $\mathbb{Z}[\mu_3]$ .

*Proof.* An irreducible proper subgroup of  $\text{SL}_{2n}(\mathbb{F}_3)$  generated by transvections is isomorphic to  $\text{Sp}_{2n}(\mathbb{F}_3)$ , cf. [KM]. The pairing on  $V$  implies that  $F$  contains  $\mu_3$ . The subgroup  $P$  of  $G$  generated by all transvections fixes  $K = \mathbb{Q}(\mu_3)$  and  $F^P$  is unramified outside  $3\infty$ , so  $F^P = K$  by Lemma 6.2. If  $V|_P$  is irreducible, then (i) holds. If  $V|_P$  is reducible, the arguments in the proofs of Lemma 2.7 and Prop. 2.8 give (ii), with  $\mathfrak{n}$  a generator for the conductor ideal of the  $\mathbb{F}[G_{\mathbb{Q}(\mu_3)}]$ -module  $W$ .  $\square$

### 3. DISCRIMINANTS OF STEM FIELDS

Let  $F/k$  be a Galois extension of number fields with group  $G$ . Let  $\mathcal{D}$  the decomposition group of a fixed prime  $\pi_F$  of  $F$  and  $\mathcal{I}_m$  the  $m^{\text{th}}$  ramification group (see §5), with  $\mathcal{I} = \mathcal{I}_0$  the inertia group. For intermediate fields  $L$ , set  $\pi_L = \pi_F \cap L$ .

**Theorem 3.1.** *Let  $G$  act transitively on  $X$ . If  $K$  is the fixed field of  $G_x$  and  $\mathcal{I}_m \backslash X$  is the set of  $\mathcal{I}_m$ -orbits of  $X$ , then*

$$\text{ord}_{\pi_k}(d_{K/k}) = \sum_{m \geq 0} \frac{1}{[\mathcal{I} : \mathcal{I}_m]} (|X| - |\mathcal{I}_m \backslash X|).$$

*Proof.* If  $H = G_x$  and  $I$  is any subgroup of  $G$ , then  $HgI \leftrightarrow Ig^{-1}x$  is a bijection between the set of double cosets  $H \backslash G / I$  and the set of orbits  $I \backslash X$ . Thus,

$$(3.2) \quad \sum_{HgI \in H \backslash G / I} [I : (I \cap H^g)] = [G : H],$$

where  $H^g = g^{-1}Hg$ . Suppose further that  $J$  is a normal subgroup of  $I$ , so that  $(I \cap H^g)J = I \cap H^gJ$  is a subgroup of  $I$ . For each  $g \in G$ , we have

$$(3.3) \quad HgI = \bigsqcup Hgz_iJ,$$

where  $z_i$  runs over a set of representatives for the right cosets  $I/(I \cap H^g)J$ . The isomorphism  $(I \cap H^g)/(J \cap H^g) \simeq (I \cap H^g)J/J$ , implies that

$$(3.4) \quad \begin{aligned} \sum_{HgI \in H \backslash G / I} \frac{|J \cap H^g|}{|I \cap H^g|} &= \sum_{HgJ \in H \backslash G / J} \frac{1}{[I : (I \cap H^g)J]} \frac{|J \cap H^g|}{|I \cap H^g|} \\ &= \sum_{HgJ \in H \backslash G / J} \frac{1}{[I : J]} = \frac{|H \backslash G / J|}{[I : J]}. \end{aligned}$$

The ramification groups for  $\pi_F$  inside  $H$  are given by  $\mathcal{I}_m \cap H$  and the different ideal  $\mathfrak{D}_{F/k}$  satisfies  $\text{ord}_{\pi_F}(\mathfrak{D}_{F/k}) = \sum_{m=0}^{\infty} (|\mathcal{I}_m| - 1)$ . By transitivity of differentials,

$$(3.5) \quad \begin{aligned} \text{ord}_{\pi_K}(\mathfrak{D}_{K/k}) &= \frac{1}{|\mathcal{I} \cap H|} \text{ord}_{\pi_F}(\mathfrak{D}_{K/k}) \\ &= \frac{1}{|\mathcal{I} \cap H|} (\text{ord}_{\pi_F}(\mathfrak{D}_{F/k}) - \text{ord}_{\pi_F}(\mathfrak{D}_{F/K})) \\ &= \sum_{m \geq 0} \frac{|\mathcal{I}_m| - |\mathcal{I}_m \cap H|}{|\mathcal{I} \cap H|}. \end{aligned}$$

Each prime of  $K$  over  $\pi_k$  has the form  $g(\pi_F) \cap K$ , corresponding to a unique double coset  $Hg\mathcal{D}$  in  $H \backslash G / \mathcal{D}$ . Since the decomposition and inertia groups of  $g(\pi_F)$  inside  $G$  are  $g\mathcal{D}g^{-1}$  and  $g\mathcal{I}g^{-1}$ , the ramification and residue degrees of  $g(\pi_F) \cap K$  over  $\pi_k$  are given by

$$(3.6) \quad e(Hg\mathcal{D}) = [\mathcal{I} : (\mathcal{I} \cap H^g)] \text{ and } f(Hg\mathcal{D}) = [\mathcal{D} : (\mathcal{D} \cap H^g)\mathcal{I}].$$

By conjugation, (3.5) implies that the exponent of  $g(\pi_F) \cap K$  in  $\mathfrak{D}_{K/k}$  is

$$(3.7) \quad x(Hg\mathcal{D}) = \sum_{m \geq 0} \frac{|\mathcal{I}_m| - |\mathcal{I}_m \cap H^g|}{|\mathcal{I} \cap H^g|}.$$

Moreover,

$$(3.8) \quad \text{ord}_{\pi_k}(d_{K/k}) = \sum_{Hg\mathcal{D} \in H \backslash G / \mathcal{D}} x(Hg\mathcal{D})f(Hg\mathcal{D}).$$

In view of (3.3) and (3.6),  $Hg\mathcal{D}$  is the disjoint union of  $f(Hg\mathcal{D})$  distinct elements of  $H \backslash G / \mathcal{I}$ . By (3.8) and (3.7), we now have

$$\text{ord}_{\pi_k}(d_{K/k}) = \sum_{Hg\mathcal{I} \in H \backslash G / \mathcal{I}} x(Hg\mathcal{D}) = \sum_{m \geq 0} \sum_{Hg\mathcal{I} \in H \backslash G / \mathcal{I}} \frac{|\mathcal{I}_m| - |\mathcal{I}_m \cap H^g|}{|\mathcal{I} \cap H^g|}.$$

But (3.2) implies that

$$\sum_{Hg\mathcal{I} \in H \backslash G/\mathcal{I}} \frac{|\mathcal{I}_m|}{|\mathcal{I} \cap H^g|} = \sum_{Hg\mathcal{I} \in H \backslash G/\mathcal{I}} \frac{[\mathcal{I} : (\mathcal{I} \cap H^g)]}{[\mathcal{I} : \mathcal{I}_m]} = \frac{[G : H]}{[\mathcal{I} : \mathcal{I}_m]} = \frac{[K : k]}{[\mathcal{I} : \mathcal{I}_m]},$$

while (3.4) with  $J = \mathcal{I}_m$  gives

$$\sum_{Hg\mathcal{I} \in H \backslash G/\mathcal{I}} \frac{|\mathcal{I}_m \cap H^g|}{|\mathcal{I} \cap H^g|} = \frac{|H \backslash G/\mathcal{I}_m|}{[\mathcal{I} : \mathcal{I}_m]}.$$

Substituting the last two identities in the previous double sum proves our claim.  $\square$

**Corollary 3.9.** *If  $\pi_k$  is tame in  $F$ , with ramification degree  $|\mathcal{I}(F/k)| = \ell$  prime, then  $\text{ord}_{\pi_k}(d_{K/k}) = (1 - \ell^{-1})(|X| - |X^{\mathcal{I}}|)$ .*

*Proof.* Thm. 3.1 implies the claim, since  $\mathcal{I}_1$  is trivial and there are  $|X^{\mathcal{I}}|$  orbits of size 1, while the others have size  $\ell$ .  $\square$

We now apply these results to semistable Galois modules  $V$  of conductor  $N$ . We write  $F = \mathbb{Q}(V)$  and  $G = \text{Gal}(F/\mathbb{Q})$ .

**Corollary 3.10.** *Let  $t = \text{ord}_p(N) \geq 1$  and  $s = \dim_{\mathbb{F}} V$ . If  $G$  acts transitively on  $X = V - \{0\}$  and  $K = F^{G_x}$ , then  $\text{ord}_p(d_{K/\mathbb{Q}}) = (1 - \ell^{-1})(q^s - q^{s-t})$ .*

*Proof.* Our claim follows from Cor. 3.9, since  $\dim V^{\mathcal{I}} = s - t$  by (1.3).  $\square$

Now assume that  $\ell = 2$  and  $V$  is symplectic of dimension  $2n$ . Let  $K$  be the fixed field of  $G_x$ , where  $G$  acts transitively on  $X$ , as below:

- i)  $G \simeq \mathcal{S}_m = \text{Sym}(X)$  and  $V$  is the representation in Remark 2.6.
- ii)  $X = \Theta_{2n}^-$  or  $X = \Theta_{2n}^- - \{\theta_0\}$ , with  $\theta_0$  fixed by  $G$ .

**Proposition 3.11.** *Let  $\mathcal{I}_v = \langle \sigma \rangle \subseteq G$  be an inertia group at  $v$  over  $p \mid N$ .*

- i) *If  $G \simeq \mathcal{S}_m$  and  $\sigma$  is the product of  $s$  disjoint transpositions, then  $\text{ord}_p(d_{K/\mathbb{Q}}) = s$  and  $\text{ord}_p(N) = \min(s, n)$ .*
- ii) *If  $G \simeq \text{Sp}_{2n}(\mathbb{F})$  or  $O_{2n}^{\pm}(\mathbb{F})$ , then  $\text{ord}_p(d_{K/\mathbb{Q}}) = \frac{1}{4}q^n(q^n - q^{n-t} - \delta)$ , with  $\delta$  as in Remark 2.10.*

*Proof.* i) Since  $|X^{\mathcal{I}_v}| = m - 2s$ , we have  $\text{ord}_p(d_{K/\mathbb{Q}}) = s$  by Cor. 3.9 and, by (1.3),  $\text{ord}_p(N) = \dim_{\mathbb{F}}(\sigma - 1)(V) = \min(s, n)$ .

ii) We give a proof for  $t = 1$ . Thus  $\sigma$  is a transvection and we choose a symplectic basis for  $V$  as in §2, such that  $\sigma = \tau_{[e_n]}$ . For the even theta characteristic  $\theta(x_1, \dots, x_{2n}) = \sum_{j=1}^n x_j x_{n+j}$ , by (2.1) and (2.2), we have

$$\sigma(\theta + a) = \theta + a + (1 + [a, e_n])e_n.$$

Thus,  $\sigma$  fixes  $\theta + a$  if and only if  $[a, e_n] = 1$ . Let  $V' = (\text{span}\{e_n, e_{2n}\})^{\perp}$  and  $\theta'(y) = \sum_{j=1}^{n-1} y_j y_{n+j}$ . Assume  $[a, e_n] = 1$  and write  $a = y + a_n e_n + e_{2n}$  with  $y$  in  $V'$ . In  $\mathbb{F}/\wp(\mathbb{F})$ , we have

$$\text{Arf}(\theta + a) = \text{Arf}(\theta) + \theta(a) = a_n + \theta'(y).$$

Hence  $\theta + a$  is in  $\Theta_{2n}^-$  precisely when one the following conditions holds:

- (a)  $a_n \in \wp(\mathbb{F})$  and  $\theta'(y) \notin \wp(\mathbb{F})$  or
- (b)  $a_n \notin \wp(\mathbb{F})$  and  $\theta'(y) \in \wp(\mathbb{F})$ .

If  $n = 1$ , only (b) applies, yielding  $\frac{1}{2}q$  choices of  $a$ . If  $n \geq 2$ ,  $y$  is in  $\wp(\mathbb{F})$  exactly when  $\theta' + y$  is in  $\Theta_{2n-2}^+$ . Hence there are  $\frac{1}{2}q|\Theta_{2n-2}^-|$  choices of  $a$  in case (a) and

$\frac{1}{2}q |\Theta_{2n-2}^+|$  choices in case (b). But  $|\Theta_{2n-2}^+| + |\Theta_{2n-2}^-| = |V'| = q^{2n-2}$  and so  $|(\Theta_{2n}^-)^{\mathcal{I}_v}| = \frac{1}{2}q^{2n-1}$ .  $\square$

**Definition 3.12.** A semistable Galois module  $V$  is *ordinary at 2* if it is symplectic and  $\mathfrak{a}^2 V = 0$ , where  $\mathfrak{a}$  is the augmentation ideal in  $\mathbb{F}[\mathcal{I}_\lambda]$  for any  $\lambda$  over 2 in  $F$ .

Let  $V$  be the Galois module of a finite flat group scheme  $\mathcal{V}$  over  $\mathbb{Z}_2$ . Then  $\mathcal{I}_\lambda$  acts trivially on  $V^m$  and  $V^{et}$ . If the biconnected subquotient  $\mathcal{V}^b$  is trivial then  $(\sigma - 1)(\sigma' - 1)(V) = 0$  for all  $\sigma, \sigma'$  in  $\mathcal{I}_\lambda$ , whence  $V$  is ordinary. If  $\mathcal{V}^b \neq 0$ , then  $\mathcal{I}_\lambda$  is not even a 2-group.

We next treat the power of 2 in  $d_{K/\mathbb{Q}}$  when  $V$  is ordinary.

**Lemma 3.13.** *We have  $\mathfrak{a}V \subseteq Z \subseteq V^{\mathcal{I}_\lambda}$  for some maximal isotropic subspace  $Z$  of  $V$ . If  $H = G_\theta$  stabilizes an odd theta characteristic  $\theta$ , then  $|\mathcal{I}_\lambda/(\mathcal{I}_\lambda \cap H)| \leq \frac{1}{2}q^n$ .*

*Proof.* Set  $\mathcal{I} = \mathcal{I}_\lambda$ . Since  $\mathfrak{a}^2 V = 0$  and  $\mathcal{I} \subseteq \text{Sp}(V)$ , we find  $\mathfrak{a}V \subseteq V^\mathcal{I} = (\mathfrak{a}V)^\perp$ . Thus,  $\mathfrak{a}V$  is contained in a maximal isotropic space  $Z$  and, by duality,  $Z \subseteq V^\mathcal{I}$ .

If  $\Gamma$  is the subgroup of  $\text{Sp}_{2n}(\mathbb{F})$  fixing both  $Z$  and  $V/Z$  pointwise, then we have  $(g - 1)(g' - 1)(V) = 0$  for all  $g, g'$  in  $\Gamma$ . Hence  $\psi(g) = (g - 1)\theta$  defines a homomorphism  $\Gamma \rightarrow V$ . In the notation of (2.1),  $\Gamma$  is generated by the transvections  $\tau_{[z]}$  with  $z$  in  $Z$ . Since we may identify  $(\tau_{[z]} - 1)\theta$  with  $\sqrt{1 + \theta(z)}z$ , the homomorphism  $\psi$  takes values in  $Z$ . We next verify the exactness of the sequence

$$(3.14) \quad 0 \rightarrow \Gamma \cap H \rightarrow \Gamma \xrightarrow{\psi} Z \xrightarrow{\theta} \mathbb{F}/\wp\mathbb{F} \rightarrow 0.$$

Since  $Z$  is isotropic,  $\theta$  is linear on  $Z$  and  $\theta$  is surjective because it is odd. Clearly  $\theta(\psi(\tau_{[z]}))$  is in  $\wp\mathbb{F}$ . Conversely, if  $\theta(z) = a^2 + a$  and  $y = (1/\sqrt{a})z$ , then  $\psi(\tau_{[y]}) = z$ . This proves exactness around  $Z$  and the rest is clear.

Finally,  $\mathcal{I} \subseteq \Gamma$  and therefore  $|\mathcal{I}/(\mathcal{I} \cap H)| \leq |\Gamma/(\Gamma \cap H)| = \frac{1}{2}q^n$ .  $\square$

**Proposition 3.15.** *If  $V$  is ordinary at 2 and  $G$  is transitive on  $\Theta_{2n}^-$  or  $\Theta_{2n}^- - \{\theta_0\}$ , then  $\text{ord}_2(d_{K/\mathbb{Q}}) \leq (q^n - 2)(q^n - 1 - \epsilon)$ , where  $\epsilon = 0$  or 1, respectively.*

*Proof.* Since  $\mathcal{I}$  is a 2-group,  $\mathcal{I}_0 = \mathcal{I}_1$ . The definition of the upper numbering (see §5) and the bound on wild ramification (1.1iii) imply that  $\mathcal{I}_2 = 1$ . By Thm. 3.1,  $\text{ord}_2(d_{K/\mathbb{Q}}) = 2(|X| - |\mathcal{I} \backslash X|)$ .

By Lemma 3.13, each  $\mathcal{I}$ -orbit of  $X$  has at most  $\frac{1}{2}q^n$  elements and there are at least  $2|\Theta_{2n}^-|/q^n = q^n - 1$  orbits when  $\epsilon = 0$ , proving the claim.

If  $\epsilon = 1$ ,  $\mathcal{I}$  fixes  $\theta_0$ . The theta characteristic  $\theta_0 + z$  is odd exactly if  $\theta_0(z)$  is in  $\wp\mathbb{F}$ . By (3.14), there are  $\frac{1}{2}q^n$  such  $z \in Z$ , giving at least  $\frac{1}{2}q^n - 1$  orbits of size 1 for  $\mathcal{I}$  acting on  $X$ . The number of orbits not accounted for is at least

$$\frac{|X| - (\frac{1}{2}q^n - 1)}{\frac{1}{2}q^n} = q^n - 2$$

and so  $|\mathcal{I} \backslash X| \geq \frac{1}{2}q^n - 1 + (q^n - 2) = \frac{3}{2}q^n - 3$ . Hence our claim.  $\square$

**Proposition 3.16.** *If  $V$  is ordinary and  $G$  is a transitive subgroup of  $\mathcal{S}_m$ , then  $\text{ord}_2(d_{K/\mathbb{Q}}) \leq 2\lfloor m/2 \rfloor$ , unless  $m = 4$  or 8, when  $\text{ord}_2(d_{K/\mathbb{Q}}) \leq 3m/2$ .*

*Proof.* We find lower bounds for the number of  $\mathcal{I}$ -orbits and apply Thm. 3.1. Since there is at least one orbit, our claims hold for  $m \leq 4$ . Assume  $m \geq 5$  and refer to the explicit representation (2.6). Let  $y_{i,j} \in Y$  denote the vector with non-zero

entries only in coordinates  $i$  and  $j$ . Write  $\bar{y} \in V$  for the coset of  $y \in Y$  when  $m$  is even and  $\bar{y} = y$  otherwise.

Suppose distinct letters  $i, j$  lie in the same  $\mathcal{I}$ -orbit. If we can find a permutation  $\sigma$  in  $\mathcal{I}$  such that  $\sigma(i) = j$  and  $\sigma(k) = k$ , then  $\bar{y}_{i,j} = (\sigma - 1)(\bar{y}_{i,k}) \in \mathfrak{a}V$  is fixed by  $\mathcal{I}$ . It follows that  $\tau(y_{i,j}) = y_{i,j}$  for all  $\tau$  in  $\mathcal{I}$  and so  $\{i, j\}$  is an  $\mathcal{I}$ -orbit.

A larger orbit can exist only if  $m = 2n + 2$  is even and  $\mathcal{I}$  contains a product of  $n + 1$  disjoint transpositions, say

$$\sigma = (1, n+2)(2, n+3) \cdots (n+1, 2n+2).$$

Treat subscripts modulo  $2n + 2$ , fix  $k$  and consider  $j \notin \{k, k+n+1\}$ . Then

$$\bar{x}_j := \bar{y}_{j,j+n+1} - \bar{y}_{k,k+n+1} = (\sigma - 1)(\bar{y}_{j,k}) \in \mathfrak{a}V$$

is fixed by  $\mathcal{I}$ . If  $m \neq 8$ ,  $\bar{x}_j$  has a unique representative  $x_j \in Y$  with exactly 4 non-zero entries and so  $\tau(x_j) = x_j$  for all  $\tau$  in  $\mathcal{I}$ . Since

$$\tau(k) \in \bigcap_{j \notin \{k, k+n+1\}} \{j, j+n+1, k, k+n+1\} = \{k, k+n+1\},$$

$\{k, k+n+1\}$  is an  $\mathcal{I}$ -orbit and every  $\mathcal{I}$ -orbit has 2 elements. If  $m = 8$ , the  $\mathcal{I}$ -orbits have size at most 4, giving the weaker bound.  $\square$

#### 4. STEM FIELD DISCRIMINANT FOR $\mathbb{Q}(A[\mathfrak{l}])$ IN A SPECIAL CASE

In this section,  $A/\mathbb{Q}$  is  $\mathfrak{o}$ -paramodular, with good reduction at 2 and  $V = A[\mathfrak{l}]$  is irreducible for some prime  $\mathfrak{l}$  of  $\mathfrak{o}$  with residue field  $\mathbb{F}_2$ . Any  $\mathfrak{o}$ -polarization of  $A$  has odd degree, since the kernel of the associated isogeny to  $\hat{A}$  intersects  $A[\mathfrak{l}]$  trivially and thus  $V = A[\mathfrak{l}]$  is symplectic for the Weil pairing. Let  $F = \mathbb{Q}(V)$  and  $G = \text{Gal}(F/\mathbb{Q})$ . The elements of  $V$  correspond to differences  $\theta_i - \theta_j$  of the 6 odd theta characteristics and we view  $G$  as a subgroup of  $\mathcal{S}_6$ , via its action on  $\Theta^-$ . Irreducibility of  $V$  implies that  $G$  has an orbit  $\Sigma \subseteq \Theta^-$  of size 5 or 6. If  $H = G_\theta$  stabilizes  $\theta$  in  $\Sigma$ , then  $K = F^H$  is a stem field for  $F$ , with  $[K : \mathbb{Q}] = |\Sigma|$ .

The following local building blocks will appear. Let  $\tilde{E} = \mathbb{Q}_2(\mu_3, \sqrt[3]{2})$  and let  $X$  be the  $G_{\mathbb{Q}_2}$ -module, 2-dimensional over  $\mathbb{F}_2$  with  $\mathbb{Q}_2(X) = \tilde{E}$ . From the exhaustive list [JR1] of 2-adic fields of low degree, or by class field theory, there is a unique quartic extension  $\tilde{M}/\mathbb{Q}_2$  whose Galois closure  $\tilde{L}$  has non-trivial tame ramification, necessarily of degree 3. Then  $\tilde{M}/\mathbb{Q}_2$  is totally ramified,  $\text{ord}_2(d_{\tilde{M}/\mathbb{Q}_2}) = 4$ ,  $\tilde{L} \supset \tilde{E}$  and  $\text{Gal}(\tilde{L}/\mathbb{Q}_2) \simeq \mathcal{S}_4$ , with inertia subgroup  $\mathcal{A}_4$ .

**Proposition 4.1.**  $\text{ord}_2(d_{K/\mathbb{Q}}) \leq 4$  (resp. 6) if  $[K : \mathbb{Q}] = 5$  (resp. 6).

*Proof.* If  $V$  is ordinary at 2, the result follows from Prop. 3.15 or 3.16. Hence we suppose  $F$  has non-trivial tame ramification over 2. Among primes over 2 in  $K$ , choose  $\lambda$  with maximal ramification degree  $e_\lambda(K)$  and consider all possibilities.

- i)  $e_\lambda(K) = 5$ . Then  $(2)\mathcal{O}_K = \lambda^5$  or  $\lambda^5\lambda'$ , depending on whether  $K$  is quintic or sextic, and  $\text{ord}_2(d_{K/\mathbb{Q}}) = 4$  by tame theory.
- ii)  $e_\lambda(K) = 3$ . If  $K$  is quintic, the worst case occurs when  $(2)\mathcal{O}_K = \lambda^3(\lambda')^2$  and then we have

$$\text{ord}_2(d_{K/\mathbb{Q}}) = \text{ord}_2(d_{K_\lambda/\mathbb{Q}_2}) + \text{ord}_2(d_{K_{\lambda'}/\mathbb{Q}_2}) = 2 + 2 = 4.$$



Suppose  $K$  is sextic. If  $(2)\mathcal{O}_K = (\lambda\lambda')^3$ , or  $\lambda^3$  with residue degree  $f_\lambda(K) = 2$ , we have  $\text{ord}_2(d_{K/\mathbb{Q}}) = 4$ . In the remaining cases, at most one more prime  $\lambda'$  over 2 ramifies in  $K$ , with  $e_{\lambda'}(K) = 2$  and we conclude as for quintics.

- iii)  $e_\lambda(K) = 4$ . Then the completion  $K_\lambda = \tilde{M}$ . If  $[K : \mathbb{Q}] = 5$ , the other prime over 2 in  $K$  is unramified, but if  $[K : \mathbb{Q}] = 6$ , there may at worst be some  $\lambda'$  with  $e_{\lambda'}(K) = 2$ . Hence

$$\text{ord}_2(d_{K/\mathbb{Q}}) \leq \begin{cases} 4 & \text{if } [K : \mathbb{Q}] = 5, \\ 4 + 2 = 6 & \text{if } [K : \mathbb{Q}] = 6. \end{cases}$$

- iv)  $e_K(\lambda) = 6$ , so  $[K : \mathbb{Q}] = 6$ ,  $(2)\mathcal{O}_K = \lambda^6$  and the inertia group  $\mathcal{I}$  of  $\lambda$  acts transitively on  $\Theta^-$ . Since a non-zero fixed point for the action of  $\mathcal{I}$  on  $V$  corresponds to a pair of theta characteristics preserved by  $\mathcal{I}$ , contradicting transitivity, there are none. The tame ramification group  $\mathcal{I}/\mathcal{I}_1$  is a cyclic subgroup of  $\mathcal{S}_6$  whose order is odd and a multiple of 3. Hence  $|\mathcal{I}/\mathcal{I}_1| = 3$ .

Because  $\mathcal{I}_1$  is a non-trivial 2-group, normal in its decomposition group  $\mathcal{D}$ , the fixed space  $W = V^{\mathcal{I}_1}$  is a non-zero  $\mathcal{D}$ -module, properly contained in  $V$ . Viewed as an  $\mathcal{I}/\mathcal{I}_1$ -module,  $W$  is semisimple. But  $\mathcal{I}/\mathcal{I}_1$  has no non-zero fixed points on  $W$ , as they would be fixed points of  $\mathcal{I}$ , so  $\dim W = 2$  and  $W \simeq X$ .

Let  $\mathcal{V} = A[l]$ , viewed as a finite flat group scheme over  $\mathbb{Z}_2$ . The multiplicative component  $\mathcal{V}^m$  cannot have order 4, since  $\mathcal{I}$  is not a 2-group, nor can it have order 2, since  $\mathcal{I}$  has no non-trivial fixed points. Hence  $\mathcal{V}^m = 0$  and  $\mathcal{V}$  is fully biconnected. There is a subgroup scheme  $\mathcal{W}$  of  $\mathcal{V}$  with  $\mathcal{D}$ -module  $W$ , and  $\mathcal{V}/\mathcal{W}$  is biconnected, so its  $\mathcal{D}$ -module also is isomorphic to  $X$ .

Schoof [Sch, Prop. 6.4] showed that if  $V$  is an extension of  $X$  by  $X$  as a  $\mathcal{D}$ -module, then  $\mathbb{Q}_2(V)$  is contained in the maximal elementary 2-extension  $\tilde{L}_1$  of  $\tilde{E}$  with ray class conductor exponent 2. One checks that  $\tilde{L}_1$  is an unramified central extension of degree 2 over  $\tilde{L}$  and the root discriminant of  $\tilde{L}_1/\mathbb{Q}_2$  is  $7/6$ . Since  $\text{ord}_2(d_{K/\mathbb{Q}})$  is even, we have  $\text{ord}_2(d_{K/\mathbb{Q}}) \leq 6$ , as claimed.  $\square$

## 5. PRESERVING THE FONTAINE BOUND

Let  $K'/K$  be a Galois extension of  $\ell$ -adic fields with Galois group  $G$ . Denote the ring of integers of  $K'$  by  $\mathcal{O}'$  and a prime element by  $\lambda'$ . Set

$$G_n = \{\sigma \in G \mid \text{ord}_{\lambda'}(\sigma(x) - x) \geq n + 1 \text{ for all } x \in \mathcal{O}'\},$$

so  $G_0$  is the inertia group and  $t_{K'/K} = [G_0 : G_1]$  is the degree of tame ramification. If  $[x] = m$ , the Herbrand function is given by

$$(5.1) \quad \varphi_{K'/K}(x) = \frac{1}{|G_0|} (|G_1| + \cdots + |G_m| + (x - m)|G_{m+1}|)$$

and is continuous and increasing. In the upper numbering of Serre [Ser1, IV],  $G^m = G_n$ , with  $m = \varphi_{K'/K}(n)$ . In the numbering of [Fo] or [JR1], this group is denoted  $G^{(m+1)}$ . Let  $\psi_{K'/K}$  be the inverse of  $\varphi_{K'/K}$ .

**Notation 5.2.** Let  $c = c_{K'/K}$  be the maximal integer such that  $G_c \neq 1$ . We omit the lower field if  $K = \mathbb{Q}_\ell$ . Let  $m_{K'} = \psi_{K'/\mathbb{Q}_\ell}(\frac{1}{\ell-1})$ .

Wild ramification in  $K'/K$  is equivalent to  $c_{K'/K} \geq 1$ . If  $G_1$  is not abelian, then  $c_{K'/K} \geq 2$ , since successive quotients in the ramification filtration are elementary abelian  $\ell$ -groups. By (5.1),  $m_{K'}$  is an integer when  $(\ell - 1)$  divides  $t_{K'/\mathbb{Q}_\ell}$ .

**Lemma 5.3.** *Let  $E \supset F$ , both Galois over  $K$ ,  $G = \text{Gal}(E/K)$  and  $H = \text{Gal}(E/F)$ . Then  $1 \rightarrow H^{\psi_{F/K}(x)} \rightarrow G^x \xrightarrow{\text{res}} \text{Gal}(F/K)^x \rightarrow 1$  is exact. In addition,*

$$(5.4) \quad m_E \geq t_{E/F} m_F \quad \text{and} \quad c_{E/K} \geq t_{E/F} c_{F/K}.$$

*Proof.* By compatibility with quotients,  $\text{res}$  is surjective and its kernel is

$$G^x \cap H = G_{\psi_{E/K}(x)} \cap H = H_{\psi_{E/K}(x)} = H^{\varphi_{E/F} \psi_{E/K}(x)} = H^{\psi_{F/K}(x)},$$

since  $\psi_{E/K} = \psi_{E/F} \psi_{F/K}$ . Thus the sequence is exact.

Def. 5.1 implies that  $t_{E/F} \varphi_{E/F}(z) \leq z$ , so  $\psi_{E/F}(z) \geq t_{E/F} z$ . If  $x = \varphi_{F/K}(c_{F/K})$ , then  $G_{\psi_{E/K}(x)} = G^x \neq 1$  by surjectivity of  $\text{res}$ . Hence

$$c_{E/K} \geq \psi_{E/K}(x) = \psi_{E/F} \psi_{F/K}(x) = \psi_{E/F}(c_{F/K}) \geq t_{E/F} c_{F/K}$$

and similarly for  $m_E \geq t_{E/F} m_F$ .  $\square$

**Definition 5.5.** Let  $F$  be the Galois closure of  $K/\mathbb{Q}_\ell$ . We say  $K$  is *Fontaine* if  $\text{Gal}(F/\mathbb{Q}_\ell)^u = 1$  for all  $u > \frac{1}{\ell-1}$ , or equivalently,  $c_F \leq m_F$ .

**Lemma 5.6.** *Let  $E \supset F$ , both Galois over  $\mathbb{Q}_\ell$ ,  $G = \text{Gal}(E/\mathbb{Q}_\ell)$  and  $H = \text{Gal}(E/F)$ .*

- i) *If  $t_{F/\mathbb{Q}_\ell} = \ell - 1$ , then  $m_E \geq t_{E/F}$ , with equality when  $G_0$  is abelian.*
- ii) *Let  $F$  be Fontaine, with non-trivial wild ramification. Then  $1 \leq c_F \leq m_F$ . Assume further that  $t_{F/\mathbb{Q}_\ell} = \ell - 1$ . Then  $c_F = m_F = 1$  and, if  $E$  is Fontaine, then  $c_E = m_E$ .*

*Proof.* i) Since  $\varphi_{F/\mathbb{Q}_\ell}(1) = \frac{1}{\ell-1}$ , we have  $m_F = 1$ , so  $m_E \geq t_{E/F}$  by (5.4). If  $G_0$  is abelian and  $t_{E/\mathbb{Q}_\ell}$  does not divide  $j$ , then  $G_j = G_{j+1}$  by [Ser1, IV, §2]. Thus the definition gives  $\varphi_{E/\mathbb{Q}_\ell}(t_{E/F}) = \frac{1}{\ell-1}$ , whence  $m_E = t_{E/F}$ .

ii) By Def. 5.5,  $\varphi_{F/\mathbb{Q}_\ell}(c_F) \leq \frac{1}{\ell-1} = \varphi_{F/\mathbb{Q}_\ell}(m_F)$ . Hence  $c_F \leq m_F$ . If  $t_{F/\mathbb{Q}_\ell} = \ell - 1$ , then  $m_F = 1$ , so  $c_F = 1$ . Surjectivity of  $\text{res}$  in Lemma 5.3 implies that  $G^{\frac{1}{\ell-1}} \neq 1$ . If  $E$  is Fontaine, it follows that  $c_E = \psi_{E/\mathbb{Q}_\ell}(\frac{1}{\ell-1}) = m_E$ .  $\square$

**Example 5.7.** By class field theory or the table of quartics [JR1], there is a unique Fontaine  $\mathcal{S}_4$ -extension  $F/\mathbb{Q}_2$ . The ramification subgroups of  $\overline{G} = \text{Gal}(F/\mathbb{Q}_2)$  are  $\overline{G}_0 \simeq \mathcal{A}_4$ ,  $\overline{G}_1 \simeq C_2^2$  and  $\overline{G}_2 = 1$ , so  $c_F = 1$ ,  $\varphi_{F/\mathbb{Q}_2}(x) = (4 + (x-1))/12$  if  $x \geq 1$  and  $m_F = 9$ . Moreover,  $E = F(i)$  remains Fontaine, with  $G = \text{Gal}(E/\mathbb{Q}_2) \simeq \mathcal{S}_4 \times C_2$ . Lemma 5.6ii may be used to show that  $|G_0| = 24$ ,  $|G_1| = 8$ ,  $|G_2| = \dots = |G_9| = 2$ ,  $|G_{10}| = 1$  and  $c_E = m_E = 9$ . Alternatively,  $E$  has two stem fields of degree 6 and this determines  $E$  uniquely in [JR1].

**Lemma 5.8.** *Let  $M/F$  be abelian, with  $F/\mathbb{Q}_\ell$  Galois. Then  $M$  is Fontaine if and only if  $F$  is Fontaine and the ray class conductor exponent  $\mathfrak{f}(M/F) \leq \lfloor m_F \rfloor + 1$ .*

*Proof.* If  $E$  is the Galois closure of  $M/\mathbb{Q}_\ell$ , then  $E/F$  is abelian and we have  $\mathfrak{f}(E/F) = \mathfrak{f}(M/F) = \varphi_{E/F}(c_{E/F}) + 1$ , cf. [Ser1, XV, §2]. The exact sequence of Lemma 5.3 with  $K = \mathbb{Q}_\ell$  implies our claim.  $\square$

**Remark 5.9.** Let  $E$  be a *number field* with root discriminant  $\varrho_E$ . Write  $\tilde{E}$  for the completion of  $E$  at a prime  $\lambda \mid \ell$  and  $e_{\tilde{E}}$  for the absolute ramification degree. Suppose  $E$  contains  $F$ , both Galois over  $\mathbb{Q}$ , with  $\tilde{E}$  Fontaine. Then

$$\text{ord}_\ell(\varrho_E) \leq 1 + \frac{1}{\ell-1} - \frac{t_{\tilde{E}/F} c_{\tilde{E}} + 1}{e_{\tilde{E}}}.$$

Indeed, if  $\mathfrak{D}_{\tilde{E}/\mathbb{Q}_\ell}$  is the different, then [Ser1, IV, Prop. 4] and [Fo, Prop. 1.3] give

$$\text{ord}_\ell(\varrho_E) = \frac{1}{e_E} \text{ord}_\lambda(\mathfrak{D}_{\tilde{E}/\mathbb{Q}_\ell}) = 1 + \varphi_{\tilde{E}/\mathbb{Q}_\ell}(c_{\tilde{E}}) - \frac{c_{\tilde{E}}+1}{e_E}.$$

Conclude by Def. 5.5 and (5.4).  $\square$

Because the upper numbering is compatible with quotients, the composition of Fontaine fields is Fontaine and there is a maximal field  $L$ , such that  $\text{Gal}(F/\mathbb{Q}_\ell)^u = 1$  for all Galois subfields  $F$  finite over  $\mathbb{Q}_\ell$  and all  $u > \frac{1}{\ell-1}$ . Since  $F = \mathbb{Q}_\ell(\mu_\ell, (1-\ell)^{\frac{1}{\ell}})$  is contained in  $L$ , Lemma 5.6ii implies a gap in the upper numbering:

$$\text{Gal}(L/\mathbb{Q}_\ell)^{\frac{1}{\ell-1}} \neq \text{Gal}(L/\mathbb{Q}_\ell)^{\frac{1}{\ell-1}+\epsilon} \text{ for } \epsilon > 0.$$

Hajir and Maier [HM] study number field extensions  $K'/K$  of *bounded depth*, i.e. with vanishing ramification groups  $\mathcal{D}_p(K'/K)^x$  for all  $x \geq \nu_p$ . When there is deep wild ramification, the concept of Galois slope content introduced by Jones and Roberts [JR1] and used in [JJ, §1.4], leads to variants of (5.4) and Remark 5.9, not required for our applications, thanks to (1.1iii).

## 6. USING ODLYZKO

We study some maximal  $(\ell, N)$ -controlled extensions  $L/\mathbb{Q}$  by means of Odlyzko's bounds [Od, Od2, DyD]. If the  $\mathbb{F}[G_\mathbb{Q}]$ -module  $V$  is semistable and bad only at  $S$ , then  $\mathbb{Q}(V)$  is  $(\ell, N_S)$ -controlled. The converse holds for  $\ell = 2$  but not for  $\ell$  odd; e.g. if  $\dim V = 2$ , then  $\text{Sym}^2 V$  rarely is semistable.

By tameness at  $p \mid N$  and the bound (1.1iii), the root discriminant of  $L/\mathbb{Q}$  satisfies  $\varrho_L < \ell^{1+\frac{1}{\ell-1}} N^{1-\frac{1}{\ell}}$ . More precisely:

$$(6.1) \quad \text{ord}_p(\varrho_L) \leq 1 - \ell^{-1} \text{ for all } p \mid N \quad \text{and} \quad \text{ord}_\ell(\varrho_L) < 1 + (\ell - 1)^{-1}.$$

**Proposition 6.2.** *For  $\ell \leq 13$ , the maximal  $(\ell, 1)$ -controlled extension  $L$  is  $\mathbb{Q}(\mu_{2\ell})$ . Under GRH, the same is true for  $\ell = 17$  and 19.*

*Proof.* For  $\ell$  odd,  $\mathbb{Q}(\mu_\ell) \subseteq L$  and  $n = [L:\mathbb{Q}]$  is a multiple of  $\ell - 1$ . From (6.1) and [Od], we find  $M$  in Table 1 below such that  $n \leq (\ell - 1)M$ . If  $\ell = 13, 17, 19$ , we see that  $M < \ell$ , so  $L/\mathbb{Q}$  is tame at  $\ell$  and  $\varrho_L \leq \ell^{1-\alpha}$ , with  $\alpha = ((\ell - 1)M)^{-1}$ . One gets a new bound  $n \leq (\ell - 1)M'$  with  $M' \leq 5$ . If  $\ell \leq 11$ , we have  $M \leq 5$ . In both cases,  $L$  is abelian over  $\mathbb{Q}(\mu_{2\ell})$  and so  $L = \mathbb{Q}(\mu_{2\ell})$  by class field theory [BK1, Lem. 2.2]. Use  $\mathbb{Q}(i) \subseteq L$  for  $\ell = 2$ .  $\square$

$\ell$	2	3	5	7	11	13	17	19
$\varrho_L \leq$	4	5.197	7.477	9.682	13.981	16.099	20.294	22.377
$M$	2	3	3	3	5	7	8	10

TABLE 1. Odlyzko bounds for  $(\ell, 1)$ -controlled fields

Now suppose  $L$  is maximal  $(2, N)$ -controlled, so  $\varrho_L < 4N^{\frac{1}{2}}$  by (6.1). If  $n = [L:\mathbb{Q}]$  is finite, [Od, Tables 3,4] provides  $B, E$ , depending on a parameter  $b$ , such that  $\varrho_L > Be^{-\frac{E}{n}}$ . In Table 2 below, we find a best bound for  $n < E/\log(B/4N^{\frac{1}{2}})$  by varying  $B > 4N^{\frac{1}{2}}$ , unconditionally for  $N \leq 21$  and under GRH for larger  $N$ .

If  $V$  is an irreducible semistable  $\mathbb{F}_2[G_\mathbb{Q}]$ -modules good outside  $S$  and  $N_S \mid N$ , then  $\text{Gal}(\mathbb{Q}(V)/\mathbb{Q})$  factors through  $\overline{G} = G/H$ , where  $H$  is the maximal normal 2-subgroup of  $G = \text{Gal}(L/\mathbb{Q})$ . For odd  $N \leq 79$  and  $N = 97$ , we find a subfield  $F$  of  $L$  containing  $L^H$  by composing a solvable extension of  $\mathbb{Q}$  with a subfield of  $\mathbb{Q}(J_0(N)[2])$ . Then we use the improvements in §5 on the bound (6.1) for  $\varrho_L$ , together with the Odlyzko tables and Magma [BCP] to control  $[L:F]$ .

$N$	3	5	7	11	13	15	17	19	21	23	29
$n \leq$	10	16	22	42	56	74	100	138	192	98	155
$N$	31	33	35	37	39	41	43	47	51	53	55
$n \leq$	181	210	244	284	330	385	449	615	852	1007	1196
$N$	57	59	61	65	67	69	71	73	77	79	97
$n \leq$	1427	1710	2061	3046	3743	4638	5800	7332	12042	15766	470652

TABLE 2. Bounds on  $n = [L:\mathbb{Q}]$  for  $(2, N)$ -controlled fields  $L$ 

**Theorem 6.3** (GRH). *Let  $V$  be semistable and irreducible over  $\mathbb{F}_2$ . If  $V$  is bad exactly over  $S$  and  $N = N_S \leq 79$  or  $N = 97$ , the following hold.*

- i) *No such  $V$  exists for  $N$  in  $\{3, 5, 7, 13, 15, 17, 21, 33, 39, 41, 55, 57, 65, 77\}$ .*
- ii)  *$V$  is unique and  $\dim V = 2$  for  $N$  in  $\{11, 19, 23, 29, 31, 35, 37, 43, 51, 53, 61\}$ .*
- iii)  *$V$  is unique for  $N$  in  $\{23, 31, 47, 71\}$ .*
- iv)  *$V$  is an irreducible  $\mathbb{F}_2[\overline{G}]$ -module with  $\overline{G} = D_9, D_3 \times \mathcal{A}_5, \mathcal{A}_5, D_3 \times D_5, \mathrm{SL}_2(\mathbb{F}_8)$  when  $N = 59, 67, 73, 79, 97$  respectively.*

**Remark 6.4.** Aside from  $\mathbb{F}_2$ , there are exactly two irreducible  $\mathbb{F}_2[\mathcal{A}_5]$ -modules, both 4-dimensional, occurring as a submodule  $V_1$  and quotient module  $V_2$  of the permutation module. The non-trivial  $\mathbb{F}_2[\mathrm{SL}_2(\mathbb{F}_8)]$ -modules have dimensions 6, 8 and 12. Further, the irreducible modules for  $G_1 \times G_2$  are the tensor products of irreducibles for  $G_1$  and  $G_2$ .

*Sketch of Proof.* In (i),  $G$  is a 2-group, except for 33, 55, 57, 77, when  $\overline{G} \simeq D_3$  has a representation whose conductor, 11 or 19, divides  $N$  properly. In (ii),  $V \simeq C_N[2]$  for an elliptic curve  $C_N$  of conductor  $N$ , except that  $V \simeq J_0(29)[\sqrt{2}]$  for  $N = 29$ . In (iii),  $V$  is the  $\mathbb{F}_2[D_h]$ -module of dimension  $h - 1$  induced by the Hilbert class field over  $\mathbb{Q}(\sqrt{-N})$  of class number  $h = 3, 3, 5, 7$  corresponding to  $N = 23, 31, 47, 71$  respectively.

**N = 59:** The two irreducibles are the constituents of  $J_0(59)[2]$ , using an equation for  $X_0(59)$ , namely  $y^2 = f(x)g(x)$  with  $f = x^3 - x^2 - x + 2$  and

$$g = x^9 - 7x^8 + 16x^7 - 21x^6 + 12x^5 - x^4 - 9x^3 + 6x^2 - 4x - 4.$$

The Galois group of  $g$  is  $D_9$  and a root of  $f$  gives a cubic subfield.

**N = 67:** Let  $V_1 = C_{67}[2]$  and  $V_2 = J_0^+(67)[2]$ . Then  $\mathrm{Gal}(\mathbb{Q}(V_2)/\mathbb{Q}) = \mathrm{SL}_2(\mathbb{F}_4)$  and  $[L:\mathbb{Q}(V_1, V_2, i)] \leq 2$ .

We provide more details for  $N = 73, 77, 79$  and 97. Let  $E$  be the maximal abelian extension of  $\mathbb{Q}$  in  $L$ . Since  $G$  is generated by involutions,  $E/\mathbb{Q}$  is the elementary 2-extension generated by  $i$  and  $\sqrt{p}$  as  $p$  ranges over  $S$ .

**Lemma 6.5.** *Let  $M \supset F$  be subfields of  $L$  containing  $E$  and Galois over  $\mathbb{Q}$ . Set  $T = \mathrm{Gal}(M/F)$  and assume  $\lambda|2$  is totally ramified of odd degree  $t = |T| > 1$  in  $M/F$ . Then  $t = 3$  and the residue degree  $f_\lambda(E/\mathbb{Q}) = 2$ .*

*Proof.* Since the image of  $\alpha: \mathrm{Gal}(M/\mathbb{Q}) \rightarrow \mathrm{Aut}(T)$  by conjugation is abelian,  $E$  contains  $M_0 = L^{\ker \alpha}$  and so  $f = f_\lambda(M_0/\mathbb{Q}) \leq f_\lambda(E/\mathbb{Q}) \leq 2$ . Any Frobenius in  $\mathcal{D}_\lambda(M/M_0)$  acts trivially on  $T$ . Thus  $2^f \equiv 1 \pmod{t}$  and the claim ensues.  $\square$

**Remark 6.6.** Let  $M \supseteq F$  be subfields of  $L$  containing  $\mathbb{Q}(i, \sqrt{N})$  and Galois over  $\mathbb{Q}$ . Denote the residue, ramification and tame degree of  $\lambda$  in  $F/\mathbb{Q}$  by  $f_0, e_0$  and  $t_0$

respectively. Given an *a priori* bound  $[M:F] \leq b$ , consider possible factorizations  $[M:F] = 2^s t_1 u_1$ , where  $2^s$  is the degree of wild ramification,  $t_1$  the degree of tame ramification and  $u_1 = f_1 g_1$  the unramified (inert and split) degree of  $\lambda$  in  $M/F$ . The resulting tame ramification in  $M/\mathbb{Q}$  requires that the completion  $M_\lambda$  contain  $\mu_{t_0 t_1}$  and so  $2^{f_0 f_1} \equiv 1 \pmod{t_0 t_1}$ .

For each  $s$  with  $0 \leq s \leq \log_2 b$ , let  $t_1 \geq 1$  run through odd integers at most  $b/2^s$ . Set  $\beta = (c_F t_1 + 1)/(2^s t_1 e_0)$ , as in Remark 5.9 and let  $n_\beta$  be the Odlyzko bound on  $[M:\mathbb{Q}]$  when  $\varrho_M \leq 2^{2-\beta} \sqrt{N}$ . Then  $1 \leq g_1 \leq n_\beta/(2^s t_1 f_1 [F:\mathbb{Q}])$ . Values of  $s, t_1, f_1$  not satisfying the congruence and inequality above are ruled out.

Let  $E_1$  be the maximal subfield of  $L$  abelian over  $E$ . By Lemmas 5.6ii and 5.8, the ray class conductor of  $E_1/E$  divides  $(1+i)^2 \mathcal{O}_E$ . Then class field theory or Magma gives Table 3 below.

$N$	$\text{Gal}(E_1/E)$	$e_\lambda(E_1/\mathbb{Q})$	$f_\lambda(E_1/\mathbb{Q})$	$g_\lambda(E_1/\mathbb{Q})$
73	$C_4$	4	2	2
77	$C_6$	6	2	4
79	$C_{15}$	2	5	6
97	$C_4$	4	2	2

TABLE 3. Decomposition type of  $\lambda|2$  in  $E_1$

$N = 73$ : The Jacobian  $J_0^+(73)$  has RM by  $\mathbb{Q}(\sqrt{5})$  and the Galois group of its 2-division field  $K$  is  $\text{SL}_2(\mathbb{F}_4) \simeq \mathcal{A}_5$ . For the 5 primes over 2 in  $K$ ,  $f_\lambda(K/\mathbb{Q}) = 3$  and Frobenius acts irreducibly on  $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_2^2$ . Since Frobenius is reducible on  $\mathcal{I}_\lambda(E_1/\mathbb{Q}) \simeq C_2^2$ , we have  $\mathcal{I}_\lambda(F/\mathbb{Q}) \simeq C_2^4$  for the compositum  $F = E_1 K$ , thus  $[F:\mathbb{Q}] = 960$ . By Table 2,  $[L:\mathbb{Q}] = 960r \leq 7332$ , so  $r \leq 7$ . Lemma 6.5 implies the tame degree  $t_\lambda(L/F) = 1$ , so  $e_\lambda(L/F)$  divides 4. Finally,  $[L:F]$  divides 4 by (6.6).

$N = 77$ : In the  $\mathcal{S}_3$ -field  $K_0 = \mathbb{Q}(J_0(11)[2]) = \mathbb{Q}(\sqrt{-11}, \theta)$ , with  $\theta^3 - 2\theta^2 + 2 = 0$ , the decomposition type over 2 is  $e_\lambda = 3$ ,  $f_\lambda = 2$ ,  $g_\lambda = 1$ . If  $K = E(\theta) = K_0(i, \sqrt{-7})$ , then  $\text{Gal}(K/\mathbb{Q}) \simeq C_2 \times C_2 \times \mathcal{S}_3$  and  $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_6$ , so  $m_K = 3$  by (5.6i). If  $F$  is the maximal subfield of  $L$  abelian over  $K$ , the ray class conductor of  $F/K$  divides  $(1+i)^4 \mathcal{O}_K = 4\mathcal{O}_K$  by Lemma 5.8. Then  $\text{Gal}(F/K) \simeq C_2 \times C_2 \times C_4$  and the decomposition type of 2 is  $e_\lambda(F/\mathbb{Q}) = 48$ ,  $f_\lambda(F/\mathbb{Q}) = 2$  and  $g_\lambda(F/\mathbb{Q}) = 4$ .

A group of order  $3 \cdot 2^a$  admits a unique quotient isomorphic to  $C_3$  or  $\mathcal{S}_3$ . If  $[L:K_0] = 3 \cdot 2^a$ , there is a  $C_3$  or  $\mathcal{S}_3$  extension of  $K_0$ . The latter provides a central quadratic  $M_0/K_0$ , with  $M_0/\mathbb{Q}$  Galois and  $\text{Gal}(M_0/\mathbb{Q}) \simeq D_6$ . In both cases, we find that  $\text{Gal}(M_0 K/K) \simeq C_3$ , contradicting  $[F:K] = 16$ .

We claim that  $\text{Gal}(L/F)$  is a 2-group. If not, since  $[L:F] \leq 31$  from Table 2 and  $[L:F] \neq 3 \cdot 2^a$ , the wild ramification degree  $|\mathcal{I}_\lambda(L/F)_1|$  divides 4. Example 5.7 and (5.4) imply that  $\mathcal{I}_\lambda(F/\mathbb{Q})_9 \neq 1$ . Use Remark 6.6 with  $c_F \geq 9$  to show that the only remaining case is  $[L:F] = 10$ , with tame degree  $t_\lambda(L/F) = 5$  and wild degree 2. It is precluded by Lemma 6.5.

Thus the kernel of the surjection  $G \xrightarrow{\eta} \text{Gal}(\mathbb{Q}(J_0(11)[2])/\mathbb{Q}) \simeq \mathcal{S}_3$  is a 2-group and irreducible representations  $V$  of  $G$  factor through  $\text{Image } \eta$ , of conductor 11, so there is no  $V$  of conductor 77.

$N = 79$ : The strict class fields  $H^\pm$  of  $\mathbb{Q}(\sqrt{\pm 79})$  have respective orders 3 and 5 and so  $E_1 = H^+ H^-$ . Let  $K^\pm$  be the maximal subfields of  $L$  abelian respectively over  $H^\pm(i)$ . Since  $e_\lambda(H^\pm(i)/\mathbb{Q}) = 2$ , the ray class conductors of  $K^\pm/H^\pm(i)$  divide

$(1+i)^2\mathcal{O}_{H^\pm(i)}$  by Lemma 5.8. Magma provides the following information.

$$\begin{aligned}\mathrm{Gal}(K^+/H^+(i)) &\simeq C_2^2 \times C_3, \text{ with } e_\lambda = 2, f_\lambda = 2, g_\lambda = 3. \\ \mathrm{Gal}(K^-/H^-(i)) &\simeq C_2^4 \times C_5, \text{ with } e_\lambda = 16, f_\lambda = 5, g_\lambda = 1.\end{aligned}$$

If  $\mathrm{Gal}(E_1/E) = \langle \tau \rangle$ , then  $\tau^5$  and  $\tau^3$  act trivially on  $K^+$  and  $K^-$  respectively. Hence  $\tau$  is trivial on  $K^+ \cap K^-$  and  $(K^+ \cap K^-)/E$  is abelian. Since  $K^+ \cap K^-$  contains  $E_1$ , equality holds by maximality of  $E_1$ . For  $F = K^+K^-$ , we therefore have  $[F : E_1] = 2^6$ ,  $[F : \mathbb{Q}] = 3840$  and  $[L : \mathbb{Q}] = 3840r$ , with  $r \leq 3$ . Because Frobenius acts irreducibly on  $\mathcal{I}_\lambda(K^-/E_1) \simeq C_2^4$  but trivially on  $\mathcal{I}_\lambda(K^+/E_1) \simeq C_2$ , we see that  $\mathcal{I}_\lambda(F/E_1) \simeq C_2^5$  and  $e_\lambda(F/\mathbb{Q}) = 64$ . By Lemma 6.5,  $t_\lambda(L/F) = 1$ , so  $[L : F] \leq 2$  by (6.6). Thus the kernel of  $G \twoheadrightarrow \mathrm{Gal}(H^+/\mathbb{Q}) \times \mathrm{Gal}(H^-/\mathbb{Q}) \simeq D_3 \times D_5$  is a 2-group.

**N = 97:** There is a subfield  $K$  of  $\mathbb{Q}(J_0(97)[2])$  with  $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{F}_8)$  and decomposition type  $e_\lambda(K/\mathbb{Q}) = 8$ ,  $f_\lambda(K/\mathbb{Q}) = 7$ ,  $g_\lambda(K/\mathbb{Q}) = 9$ . Any Frobenius in  $\mathcal{D}_\lambda(K/\mathbb{Q})$  acts irreducibly on  $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_2^3$  but reducibly on  $\mathcal{I}_\lambda(E_1/\mathbb{Q}) \simeq C_2^2$ , so  $\mathcal{I}_\lambda(F/\mathbb{Q}) \simeq C_2^5$  for the compositum  $F = E_1K$ . Since  $[F : \mathbb{Q}] = 504 \cdot 16 = 8064$ , Table 2 implies that  $[L : F] \leq 58$ . Thus the dimensions of irreducible representations of  $\mathrm{SL}_2(\mathbb{F}_8)$  over  $\mathbb{F}_p$  for small  $p$  force the action of  $\mathrm{Gal}(F/E_1)$  on the maximal abelian quotient of  $\mathrm{Gal}(L/F)$  to be trivial. But no central extension of  $\mathrm{SL}_2(\mathbb{F}_8)$  is perfect [Asch, HBI]. Hence  $L$  is the compositum of  $F$  with a solvable extension of  $E_1$ . The ray class extension of  $E_1$  whose conductor divides  $\prod \lambda^2$ , as  $\lambda$  runs over the primes above 2 in  $\mathcal{O}_{E_1}$ , turns out to be trivial, whence  $L = F$  by Lemmas 5.6ii and 5.8.  $\square$

**N = 127:** We begin the solvable tower with  $E_0 = E = \mathbb{Q}(i, \sqrt{127})$  and find successive maximal abelian extensions  $E_{j+1}/E_j$  in  $L/\mathbb{Q}$ . For ray class conductor  $(1+i)^2\mathcal{O}_E$ , we have  $[E_1 : E] = 5$ . Thus  $E_1$  is the compositum of  $\mathbb{Q}(i)$  and the Hilbert class field over  $\mathbb{Q}(\sqrt{-127})$ . Now  $e_\lambda(E_1/\mathbb{Q}) = 2$ , so the ray class conductor of  $E_2/E_1$  divides  $(1+i)^2\mathcal{O}_{E_1}$  and we have  $\mathrm{Gal}(E_2/E_1) = C_2^4$ . Moreover, any Frobenius in  $\mathcal{D}_\lambda(E_2/\mathbb{Q})$  has irreducible action of order 5 on this ray class group. The decomposition type over 2 is  $e_\lambda(E_2/\mathbb{Q}) = 32$ ,  $f_\lambda(E_2/\mathbb{Q}) = 5$ ,  $g_\lambda(E_2/\mathbb{Q}) = 2$ . The ray class conductor of  $E_3/E_2$  divides  $\prod \lambda^2$ , as  $\lambda$  runs over the primes of  $\mathcal{O}_{E_2}$  above 2, but we do not know whether  $E_3 = E_2$ .

There is a subfield  $K$  of  $\mathbb{Q}(J_0(127)[2])$  with  $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{F}_8)$  and decomposition type  $e_\lambda(K/\mathbb{Q}) = 8$ ,  $f_\lambda(K/\mathbb{Q}) = 7$ ,  $g_\lambda(K/\mathbb{Q}) = 9$ . Any Frobenius in  $\mathcal{D}_\lambda(K/\mathbb{Q})$  has irreducible action of order 7 on  $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_2^3$ . For the compositum  $F = E_2K$ , of degree  $320 \cdot 504 = 161280$ , we therefore have  $\mathcal{I}_\lambda(F/\mathbb{Q}) \simeq C_2^8$  and so  $c_F = m_F = 1$  by Lemma 5.6. By Remark 5.9, the root discriminant is  $\varrho_F = 2^{2-\frac{1}{128}}\sqrt{127} \approx 44.834$ . Since this just exceeds the asymptotic bound  $8\pi e^\gamma \approx 44.763$ , where  $\gamma$  is Euler's constant [Od2], we do not know whether  $[L : \mathbb{Q}]$  is finite and thus it would be entertaining to find  $L$ .

## 7. SOME SPECULATIONS

Assume  $\ell \nmid N$  is prime. Let  $\mathrm{AB}(N)$  be the set of simple semistable abelian varieties  $A$  with  $N_A|N$  and let  $\mathrm{Irr}(\ell, N)$  be the set of irreducible semistable  $\mathbb{F}_\ell[G_\mathbb{Q}]$ -modules  $V$  with  $N_V|N$ , both taken up to isomorphism.

- Q1.** Is  $\mathrm{AB}(N)$  finite?
- Q2.** Is  $\mathrm{Irr}(\ell, N)$  finite?
- Q3.** Is  $\log N_A \gg g \log g$  as  $g = \dim A \rightarrow \infty$ ?

Faltings' theorem answers **Q1** in the affirmative if  $\dim A$  is bounded in terms of  $N_A$ . Mestre [Mes] shows that standard *conjectures* on Hasse-Weil L-functions imply that  $\dim A \leq .42 \log N_A$ , without assuming semistability or simplicity. Such strong modularity or even an answer to **Q2** are equally unavailable. However, the negation of **Q1** violates one of the following two *plausible* assertions.

**P<sub>1</sub>**( $\ell, N$ ). The dimension of the composition factors of  $A[\ell]$  is bounded for  $A$  in  $\text{AB}(N)$ .

**P<sub>2</sub>**( $\ell, N$ ). The number of isomorphism classes of composition factors of  $A[\ell]$  of conductor 1 and  $\mathbb{F}_\ell$ -dimension at least 2 is bounded for  $A$  in  $\text{AB}(N)$ .

Prop. 6.2 asserts that **P<sub>2</sub>**( $\ell, N$ ) necessarily holds for small  $\ell$ .

**Proposition 7.1.** *Assume **P<sub>1</sub>**( $\ell, N$ ) and **P<sub>2</sub>**( $\ell, N$ ). Then  $\text{AB}(N)$  is finite.*

*Proof.* We shall denote by  $\beta_i$  constants depending only on  $\ell$  and  $N$ . Suppose  $A$  in  $\text{AB}(N)$  is good at  $\ell$ . Write  $\epsilon_0(A[\ell])$  for the number of 1-dimensional constituents of  $A[\ell]$ ,  $\mathfrak{S}_\ell(A)$  for the multiset of other irreducible constituents  $E$  and  $m_E = \dim_{\mathbb{F}_\ell} E$ . Let  $\mathfrak{S}_\ell^1(A)$  be the multiset of those  $E$  in  $\mathfrak{S}_\ell(A)$  with conductor  $N_E = 1$ . We assume that  $m_E \leq \beta_1$  and  $|\mathfrak{S}_\ell^1(A)| \leq \beta_2$  as  $A$  varies in  $\text{AB}(N)$ . We have

$$(7.2) \quad 2 \dim A = \dim A[\ell] = \epsilon_0(A[\ell]) + \sum_{E \in \mathfrak{S}_\ell^1(A)} m_E + \sum_{N_E > 1} m_E.$$

We bound the last two sums by  $\beta_3 = \beta_1(\beta_2 + \Omega(N_A))$ , where  $\Omega(n) = \sum_p \text{ord}_p(n)$ . Theorem 5.3 of [BK2] implies that

$$\epsilon_0(A[\ell]) \leq 2\Omega(N_A) + \sum_{E \in \mathfrak{S}_\ell(A)} \delta_A(E),$$

where  $\delta_A(E)$  is bounded in terms of  $N$ ,  $\ell$  and the strict class number  $h_E$  of  $F = \mathbb{Q}(E)$ , thanks to [BK2, 4.3.8, 4.3.13, 4.4.1]. If  $m = \dim E$ , then  $n = [F : \mathbb{Q}] \leq |\text{GL}_m(\mathbb{F}_\ell)| < \ell^{m^2}$ . Hence the discriminant of  $F$  satisfies  $\log |d_{F/\mathbb{Q}}| \leq n(2 \log \ell + \log N_E)$  by (6.1). An upper bound on the residue of the zeta function [Lou] and a lower bound on the regulator [Sko] show that  $h_E \leq \beta_4$ . Thus  $\delta_A(E) \leq \beta_5$  and  $\epsilon_0(A[\ell]) \leq 2\Omega(N_A) + \beta_5(\beta_2 + \Omega(N_A))$ .  $\square$

**Proposition 7.3** (GRH). *If  $N \leq 15683$  is odd and squarefree, then  $\dim V$  is bounded for  $V$  in  $\text{Irr}(N, 2)$  and  $\text{AB}(N)$  is finite.*

*Proof.* Prop. 2.8 restricts the group  $G = \text{Gal}(\mathbb{Q}(V)/\mathbb{Q})$  and Cor. 3.10, 3.11 estimate the discriminant of a stem field  $K$ . If  $\dim V$  is bounded, then the finiteness of  $\text{AB}(N)$  ensues from Prop. 7.1. Otherwise the root discriminants  $\varrho_K$  have an asymptotic upper bound of  $4N^{1/4}$  and a lower bound of  $8\pi e^\gamma$  and so  $N > 15683$ .  $\square$

**Remark 7.4.** Unconditionally, if  $N$  is squarefree,  $V$  is in  $\text{Irr}(N, 2)$  and

$$2 \dim V + 1 \geq \max(7, 3.06 \log N),$$

then  $G = \text{Gal}(\mathbb{Q}(V)/\mathbb{Q})$  can only be  $Q$  or  $Q \wr \mathcal{S}_2$  with  $Q = O^\pm(V)$ ,  $\text{Sp}(V)$  or  $\text{SL}(V)$ . Otherwise,  $G = \mathcal{S}_m$  or  $\mathcal{S}_m \wr \mathcal{S}_2$ , with  $m = 2 \dim V + 1$  or  $2 \dim V + 2$ , as in Rem. 2.6. By Cor. 3.11i, the root discriminant of a stem field for  $\mathbb{Q}(V)$  is at most  $4N^{1/m}$ , while it is at least 5.548 when  $m \geq 7$  by [DyD].

## REFERENCES

- [Asch] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986.
- [BCP] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system. I. The user language. *J. Symb. Comp.*, **24**, (1997) 235–265.
- [BK1] A. Brumer and K. Kramer, Semistable Abelian varieties with small division fields. *Galois Theory and Modular Forms*, Hashimoto, Miyake, Nakamura, eds., Kluwer, 2003 13–38.
- [BK2] A. Brumer and K. Kramer, Paramodular abelian varieties of odd conductor, arXiv:1004.4699.
- [DyD] F. Diaz y Diaz, Tables minorant la racine  $n$ -ième du discriminant d'un corps de degré  $n$ , Ph.D. Thesis, Publ. Math. Orsay, 1980.
- [Dye] R.H. Dye, Interrelations of symplectic and orthogonal groups in characteristic two, *J. of Algebra*, **59**, (1979) 202–221.
- [Fo] J.-M. Fontaine, Il n'y a pas de variété abélienne sur  $\mathbb{Z}$ , *Invent. Math.* **81**, (1985) 515–538.
- [GH] B. H. Gross and J. Harris, On some geometric constructions related to theta characteristics. *Contributions to automorphic forms, geometry, and number theory*, Hida et al, eds., Johns Hopkins, (2004) 279–312.
- [Gro] A. Grothendieck, Modèles de Néron et monodromie. Sémin. de Géom. 7, Exposé IX, Lecture Notes in Math., **288**, Springer-Verlag, 1973.
- [HM] F. Hajir and C. Maire, Extensions of number fields with wild ramification of bounded depth, *Inter. Math. Res. Notices*, **13**, (2002) 667–696.
- [HBI] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.
- [JJ] J. Jones, Wild ramification bounds and simple group Galois extensions ramified only at 2, *Proc. Amer. Math. Soc.*, **139**, (2011), 807–821.
- [JR1] J. Jones and D. Roberts, Local Fields, *J. Symbolic Computation*, **41**(1), (2006) 80–97.
- [JR2] J. Jones and D. Roberts, Galois number fields with small root discriminant, *J. Number Theory*, **122**, (2007) 379–407.
- [Kan] W.M. Kantor, Subgroups of classical groups generated by long roots, *Trans. Amer. Math. Soc.*, **248**, (1979) 347–379.
- [KM] G. Kemper and G. Malle, The finite irreducible linear groups with polynomial ring of invariants, *Transformation Groups*, **2**, (1997) 57–89.
- [Lou] S. Louboutin, Explicit Upper Bounds for Residues of Dedekind Zeta Functions . . . , *Canad. J. Math.*, **53**(6), (2001) 1194–1222.
- [McL] J. McLaughlin, Some subgroups of  $SL_n(\mathbb{F}_2)$ , *Ill. J. Math.* **13**, (1969) 108–115.
- [Mes] J.-F. Mestre, Formules explicites et minoration de conducteurs de variétés algébriques, *Compositio Math.*, **58**, (1982) 209–232.
- [Od] A. Odlyzko, Lower bounds for discriminants of number fields II, *Tôhoku Math. JI.* **29**, (1977) 209–216. <http://www.dtc.umn.edu/~odlyzko/unpublished/index.html>.
- [Od2] A. Odlyzko, Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Sém. Théorie Nombres Bordeaux*, **(2)2**(1), (1990) 119–141.
- [Sch] R. Schoof, Abelian varieties over cyclotomic fields with everywhere good reduction, *Math. Ann.*, **325**, (2003) 413–448.
- [Sko] N.-P. Skorrupa, Quick lower bounds for regulators of number fields, *Ens. Math.*, **39**, (1993) 137–141.
- [Ser0] J.-P. Serre, Minorations de discriminants, note of October 1975, *OEuvres*, **3**, Springer, 1986, 240–243.
- [Ser1] J.-P. Serre, *Local Fields*, Lecture Notes in Math., **67**, Springer-Verlag 1979.
- [Zal1] A. E. Zaleskii and V. N. Serežkin, Finite linear groups generated by reflections, *Math. USSR Izv.*, **17**, (1981) 477–503.

DEPARTMENT OF MATHEMATICS, FORDHAM UNIVERSITY, BRONX, NY 10458

*E-mail address*: `brumer@fordham.edu`

DEPARTMENT OF MATHEMATICS, QUEENS COLLEGE AND THE GRADUATE CENTER (CUNY),  
65-30 KISSENA BOULEVARD, FLUSHING, NY 11367, FLUSHING, NY 11367

*E-mail address*: `kkramer@gc.cuny.edu`